24.03.2023

Correctly erasing your data to dispose or pass on your device

Simply deleting the content on a device is not enough. Attackers can gain access to user accounts via disposed or resold devices on which data has 'only' been deleted.

Electronic data remains on the storage medium even after deletion or emptying the recycle bin. Only the information on the storage location in the internal table of contents of the hard disk is deleted. For the final destruction of the data, the storage location of the information must be overwritten several times and randomly. Dedicated programs are available for this process. When used correctly, the hard disk is reliably erased so that data cannot be recovered even with recovery tools.

Before erasing, you should remove linked accounts (Apple account, Office 365 account, etc.) from your device and log out of all applications.

Modern operating systems have dedicated functions to reset the computer or mobile device and prepare it for disposal or resale. However, to achieve a reliable deletion of your data on a hard disk, it is recommended to additionally randomly overwrite the hard disk several times with a specialized program. The recovery data of the device manufacturer should also be overwritten in the process.

If the device is not to be used further, a physical destruction of the data media can also be carried out. However, the storage devices must first be removed from the device, which can be time-consuming.

For further information on this topic, see our article "Secure deletion" (https://www.ebas.ch/en/secure-deletion/) .